What is quantum computing?

Quantum computing is an emergent field of cutting-edge computer science harnessing the unique qualities of quantum mechanics to solve problems beyond the ability of even the most powerful classical computers.

The field of quantum computing contains a range of disciplines, including quantum hardware and quantum algorithms. While still in development, quantum technology will soon be able to solve complex problems that supercomputers can't solve, or can't solve fast enough.

By taking advantage of quantum physics, fully realized quantum computers would be able to process massively complicated problems at orders of magnitude faster than modern machines. For a quantum computer, challenges that might take a classical computer thousands of years to complete might be reduced to a matter of minutes.

The study of subatomic particles, also known as quantum mechanics, reveals unique and fundamental natural principles. Quantum computers harness these fundamental phenomena to compute probabilistically and quantum mechanically.

Four key principles of quantum mechanics

Understanding quantum computing requires understanding these four key principles of quantum mechanics:

- **Superposition:** Superposition is the state in which a quantum particle or system can represent not just one possibility, but a combination of multiple possibilities.
- **Entanglement:** Entanglement is the process in which multiple quantum particles become correlated more strongly than regular probability allows.
- **Decoherence:** Decoherence is the process in which quantum particles and systems can decay, collapse or change, converting into single states measurable by classical physics.
- **Interference:** Interference is the phenomenon in which entangled quantum states can interact and produce more and less likely probabilities.

Qubits

While classical computers rely on binary bits (zeros and ones) to store and process data, quantum computers can encode even more data at once using quantum bits, or qubits, in superposition.

A qubit can behave like a bit and store either a zero or a one, but it can also be a weighted combination of zero and one at the same time. When

combined, qubits in superposition can scale exponentially. Two qubits can compute with four pieces of information, three can compute with eight, and four can compute with sixteen.

However, each qubit can only output a single bit of information at the end of the computation. Quantum algorithms work by storing and manipulating information in a way inaccessible to classical computers, which can provide speedups for certain problems.

As silicon chip and superconductor development has scaled over the years, it is distinctly possible that we might soon reach a material limit on the computing power of classical computers. Quantum computing could provide a path forward for certain important problems.

With leading institutions such as IBM, Microsoft, Google and Amazon joining eager startups such as Rigetti and Ionq in investing heavily in this exciting new technology, quantum computing is estimated to become a USD 1.3 trillion industry by 2035.[1]

Turn good intentions into action

The weekly Think newsletter provides access to news and research on sustainability, AI and more.

Subscribe today

How do quantum computers work?

A primary difference between classical and quantum computers is that quantum computers use qubits instead of bits to store exponentially more information. While quantum computing does use binary code, qubits process information differently from classical computers. But what are qubits and where do they come from?

What are qubits?

Generally, qubits are created by manipulating and measuring quantum particles (the smallest known building blocks of the physical universe), such as photons, electrons, trapped ions and atoms. Qubits can also engineer systems that behave like a quantum particle, as in superconducting circuits.

To manipulate such particles, qubits must be kept extremely cold to minimize noise and prevent them from providing inaccurate results or errors resulting from unintended decoherence.

There are many different types of qubits used in quantum computing today, with some better suited for different types of tasks.

A few of the more common types of qubits in use are as follows:

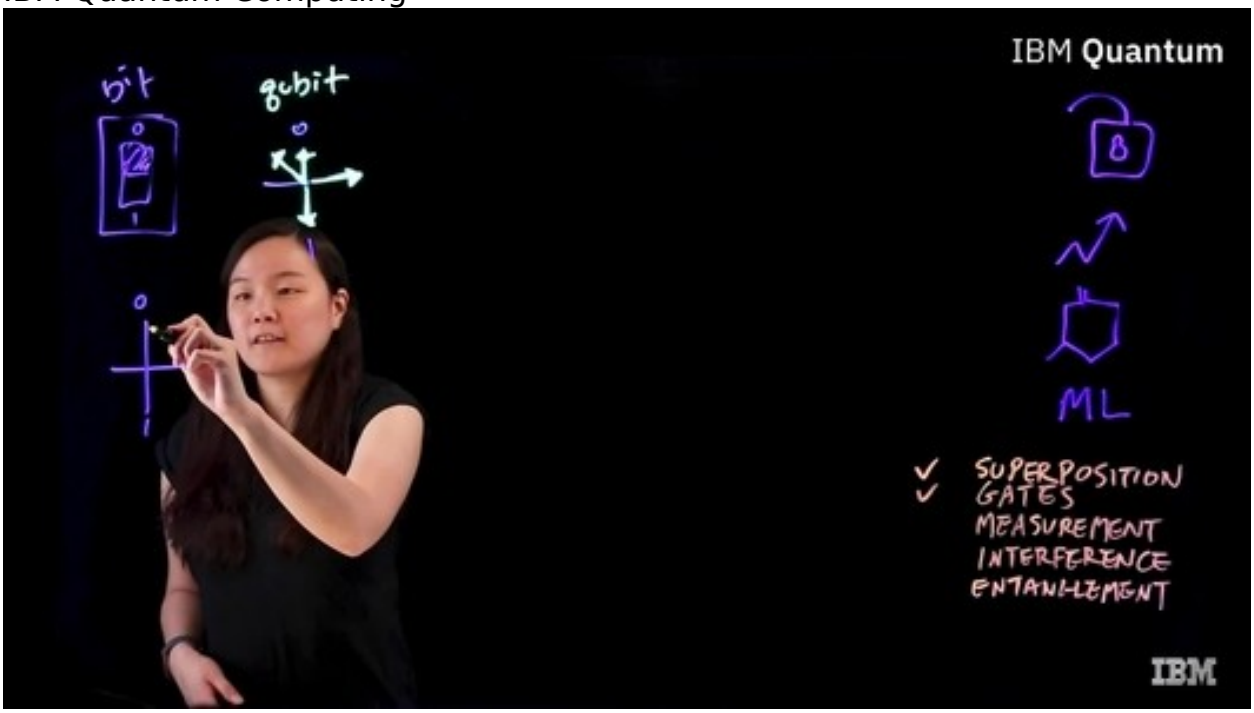
- **Superconducting qubits:** Made from superconducting materials operating at extremely low temperatures, these qubits are favored for their speed in performing computations and fine-tuned control.
- **Trapped ion qubits:** Trapped ion particles can also be used as qubits and are noted for long coherence times and high-fidelity measurements.
- **Quantum dots:** Quantum dots are small semiconductors that capture a single electron and use it as a qubit, offering promising potential for scalability and compatibility with existing semiconductor technology.
- **Photons:** Photons are individual light particles used to send quantum information across long distances through optical fiber cables and are currently being used in quantum communication and quantum cryptography.
- **Neutral atoms:** Commonly occurring neutral atoms charged with lasers are well suited for scaling and performing operations.

When processing a complex problem, such as factoring large numbers, classical bits become bound up by holding large quantities of information. Quantum bits behave differently. Because qubits can hold a superposition, a

quantum computer that uses qubits can approach the problem in ways different from classical computers.

As a helpful analogy for understanding how quantum computers use qubits to solve complicated problems, imagine you are standing in the center of a complicated maze. To escape the maze, a traditional computer would have to “brute force” the problem, trying every possible combination of paths to find the exit. This kind of computer would use bits to explore new paths and remember which ones are dead ends.

Comparatively, a quantum computer might derive a bird’s-eye view of the maze, testing multiple paths simultaneously and using quantum interference to reveal the correct solution. However, qubits don't test multiple paths at once; instead, quantum computers measure the probability amplitudes of qubits to determine an outcome. These amplitudes function like waves, overlapping and interfering with each other. When asynchronous waves overlap, it effectively eliminates possible solutions to complex problems, and the realized coherent wave or waves present the solution.
IBM Quantum Computing



What is Quantum Computing?
What is a quantum computer? How is it different from classical computing? In this video, Jessie Yu explains the five key elements of a quantum computer and the implications for quantum computing.
Explore Quantum_

Key principles of quantum computing

When discussing quantum computers, it is important to understand that quantum mechanics is not like traditional physics. The behaviors of quantum particles often appear to be bizarre, counterintuitive or even impossible. Yet the laws of quantum mechanics dictate the order of the natural world.

Describing the behaviors of quantum particles presents a unique challenge. Most common-sense paradigms for the natural world lack the vocabulary to communicate the surprising behaviors of quantum particles.

To understand quantum computing, it is important to understand a few key terms:

- Superposition
- Entanglement
- Decoherence
- Interference.

Superposition

A qubit itself isn't very useful. But it can place the quantum information it holds into a state of superposition, which represents a combination of all possible configurations of the qubit. Groups of qubits in superposition can create complex, multidimensional computational spaces. Complex problems can be represented in new ways in these spaces.

This superposition of qubits gives quantum computers their inherent parallelism, allowing them to process many inputs simultaneously.

Entanglement

Entanglement is the ability of qubits to correlate their state with other qubits. Entangled systems are so intrinsically linked that when quantum processors measure a single entangled qubit, they can immediately determine information about other qubits in the entangled system.

When a quantum system is measured, its state collapses from a superposition of possibilities into a binary state, which can be registered like binary code as either a zero or a one.

Decoherence

Decoherence is the process in which a system in a quantum state collapses into a nonquantum state. It can be intentionally triggered by measuring a quantum system or by other environmental factors (sometimes these factors trigger it unintentionally). Decoherence allows quantum computers to provide measurements and interact with classical computers.

Interference

An environment of entangled qubits placed into a state of collective superposition structures information in a way that looks like waves, with

amplitudes associated with each outcome. These amplitudes become the probabilities of the outcomes of a measurement of the system. These waves can build on each other when many of them peak at a particular outcome, or cancel each other out when peaks and troughs interact. Amplifying a probability or canceling out others are both forms of interference.

How the principles work together

To better understand quantum computing, consider that two counterintuitive ideas can both be true. The first is that objects that can be measured—qubits in superposition with defined probability amplitudes—behave randomly. The second is that objects too distant to influence each other—entangled qubits—can still behave in ways that, though individually random, are somehow strongly correlated.

A computation on a quantum computer works by preparing a superposition of computational states. A quantum circuit, prepared by the user, uses operations to generate entanglement, leading to interference between these different states, as governed by an algorithm. Many possible outcomes are canceled out through interference, while others are amplified. The amplified outcomes are the solutions to the computation.

Classical computing versus quantum computing

Quantum computing is built on the principles of quantum mechanics, which describe how subatomic particles behave differently from macrolevel physics. But because quantum mechanics provides the foundational laws for our entire universe, on a subatomic level, every system is a quantum system.

For this reason, we can say that while conventional computers are also built on top of quantum systems, they fail to take full advantage of the quantum mechanical properties during their calculations. Quantum computers take better advantage of quantum mechanics to conduct calculations that even high-performance computers cannot.

What is a classical computer?

From antiquated punch-card adders to modern supercomputers, traditional (or classical) computers essentially function in the same way. These machines generally perform calculations sequentially, storing data by using binary bits of information. Each bit represents either a 0 or 1.

When combined into binary code and manipulated by using logic operations, we can use computers to create everything from simple operating systems to the most advanced supercomputing calculations.

What is a quantum computer?

Quantum computers function similarly to classical computers, but instead of bits, quantum computing uses qubits. These qubits are special systems that act like subatomic particles made of atoms, superconducting electric circuits or other systems that data in a set of amplitudes applied to both 0 and 1, rather than just two states (0 or 1). This complicated quantum mechanical concept is called a superposition. Through a process called quantum entanglement, those amplitudes can apply to multiple qubits simultaneously.

The difference between quantum and classical computing

Classical computing

- Used by common, multipurpose computers and devices.
- Stores information in bits with a discrete number of possible states, 0 or 1.
- Processes data logically and sequentially.

Quantum computing

- Used by specialized and experimental quantum mechanics-based quantum hardware.
- Stores information in qubits as 0, 1 or a superposition of 0 and 1.
- Processes data with quantum logic at parallel instances, relying on interference.

Quantum processors do not perform mathematical equations the same way classical computers do. Unlike classical computers that must compute every step of a complicated calculation, quantum circuits made from logical qubits can process enormous datasets simultaneously with different operations, improving efficiency by many orders of magnitude for certain problems.

Quantum computers have this capability because they are probabilistic, finding the most likely solution to a problem, while traditional computers are deterministic, requiring laborious computations to determine a specific singular outcome of any inputs.

While traditional computers commonly provide singular answers, probabilistic quantum machines typically provide ranges of possible answers. This range might make quantum seem less precise than traditional computation; however, for the kinds of incredibly complex problems quantum computers might one day solve, this way of computing could potentially save hundreds of thousands of years of traditional computations.

While fully realized quantum computers would be far superior to classical computers for certain kinds of problems requiring large data sets or for completing other problems like advanced prime factoring, quantum computing is not ideal for every, or even most problems.

Realistically, classical computers will continue to be used for the majority of their current applications. However, cloud-connected quantum computers or hybrid ecosystems are already being implemented to explore a wide array of

advanced applications. As quantum computing continues to progress, we can expect this advanced technology to not only impact existing industries, but potentially unlock entire new ones as well.

When is quantum computing superior?

For most kinds of tasks and challenges, traditional computers are expected to remain the best solution. But when scientists and engineers encounter certain very complex problems, that's where quantum comes into play. For these types of difficult calculations, even the most powerful supercomputers (big machines with thousands of traditional cores and processors) pale in comparison to quantum computing's power. That's because even supercomputers are binary code-based machines reliant on 20th-century transistor technology. Classical computers are simply unable to process such complex problems.

Complex problems are problems with lots of variables interacting in complicated ways. Modeling the behavior of individual atoms in a molecule is a complex problem, because of all the different electrons interacting with one another. Identifying new physics in a supercollider is also a complex problem. There are some complex problems that we do not know how to solve with classical computers at any scale.

A classical computer might be great at difficult tasks like sorting through a big database of molecules. But it struggles to solve more complex problems, like simulating how those molecules behave. Today, if scientists want to know how a molecule will behave, they must synthesize it and experiment with it in the real world. If they want to know how a slight tweak would impact its behavior, they usually need to synthesize the new version and run their experiment all over again. This is an expensive, time-consuming process that impedes progress in fields as diverse as medicine and semiconductor design.

A classical supercomputer might try to simulate molecular behavior with brute force, by using its many processors to explore every possible way every part of the molecule might behave. But as it moves past the simplest, most straightforward molecules available, the supercomputer stalls. No computer has the working memory to handle all the possible permutations of molecular behavior by using any known methods.

Quantum algorithms take a new approach to these sorts of complex problems—creating multidimensional computational spaces or running calculations that behave much like these molecules themselves. This turns out to be a much more efficient way of solving complex problems like chemical simulations.

Engineering firms, financial institutions and global shipping companies—among others—are exploring use cases where quantum computers could solve important problems in their fields. An explosion of benefits from quantum research and development is taking shape on the horizon. As quantum hardware scales and quantum algorithms advance, many big, important problems like molecular simulation should find solutions.

Quantum computing use cases

First theorized in the early 1980s, it wasn't until 1994 that MIT mathematician Peter Shor published one of the first practical real-world applications for a quantum machine. Shor's algorithm for integer factorization demonstrated how a quantum mechanical computer could potentially break the most advanced cryptography systems of the time—some of which are still used today. Shor's findings demonstrated a viable application for quantum systems, with dramatic implications for not just cybersecurity, but many other fields.

Quantum computers excel at solving certain complex problems with the potential to speed up the processing of large-scale data sets. From the development of new drugs and performing machine learning in a new way to supply-chain optimization and climate change challenges, quantum computing might hold the key to breakthroughs in a number of critical industries.

Pharmaceuticals

Quantum computers capable of simulating molecular behavior and biochemical reactions could massively speed up the research and development of life-saving new drugs and medical treatments.

Chemistry

For the same reasons quantum computers could impact medical research, they might also provide undiscovered solutions for mitigating dangerous or destructive chemical byproducts. Quantum computing could lead to improved catalysts that enable petrochemical alternatives or better processes for the carbon breakdown necessary for combating climate-threatening emissions.

Machine learning

As interest and investment in artificial intelligence (AI) and related fields like machine learning ramps up, researchers are pushing AI models to new extremes, testing the limits of our existing hardware and demanding tremendous energy consumption. There is evidence that some quantum algorithms might be able to look at datasets in a new way, providing a speedup for some machine learning problems.

Quantum advantage versus quantum utility

While no longer simply theoretical, quantum computing is still under development. As scientists around the world strive to discover new techniques to improve the speed, power and efficiency of quantum

machines, technology is approaching a turning point. We understand the evolution of useful quantum computing using the concepts of quantum advantage and quantum utility.

Quantum utility

Quantum utility refers to any quantum computation that provides reliable, accurate solutions to problems that are beyond the reach of brute force classical computing quantum-machine simulators. Previously, these problems were accessible only to classical approximation methods—usually problem-specific approximation methods carefully crafted to exploit the unique structures of a given problem.

Quantum advantage

Broadly defined, the term quantum advantage refers to a hypothetical quantum computer capable of outperforming all classical supercomputer methods for some problem, even approximate methods. A quantum computer capable of achieving the quantum advantage should be able to deliver a significant, practical benefit beyond all known classical computing methods—calculating solutions in a way that is cheaper, faster or more accurate than any available classical alternatives.

Quantum benchmarks

Because quantum computing now offers a viable alternative to classical approximation for certain problems, researchers say it is a useful tool for scientific exploration, or that it has utility. Quantum utility does not constitute a claim that quantum methods have achieved a proven speed-up over all known classical methods. This is a key difference from the concept of quantum advantage.

In 2019, leading researchers on the IBM Quantum team invented a metric known as quantum volume to assign a singular, calculable measurement of a quantum computer’s ability.

Quantum volume measures the largest quantum circuit that can pass a quantum volume test. The quantum volume test asks the quantum computer to run circuit with random gates and measures how often the circuits output the expected outcomes. However, as we continue scaling up quantum processors, it’s becoming clear that we need more than just quantum volume to fully encapsulate the performance of utility-scale quantum computers.

While quantum volume is still one of a few ways in which we can measure errors within a quantum system, the IBM team introduced two additional metrics to better benchmark quantum computers, layer fidelity and circuit layer operations per second (CLOPS).

Layer fidelity

An extremely valuable benchmark, layer fidelity provides a way to encapsulate the entire quantum processor's ability to run circuits while revealing information about individual qubits, gates and crosstalk. By running the layer fidelity protocol, researchers can qualify the overall quantum device, while also gaining access to granular performance and error information about individual components.

Quantum processing speed

In addition to layer fidelity, IBM also defined a speed metric, circuit layer operations per second (CLOPS). Currently, CLOPS is a measure of how quickly our processors can run quantum volume circuits in series, acting as a measure of holistic system speed incorporating quantum and classical computing.

Together, layer fidelity and CLOPS provide a new way to benchmark systems that's more meaningful to the people trying to improve and use our hardware. These metrics will make it easier to compare systems to one another, to compare our systems to other architectures, and to reflect performance gains across scales.

Making quantum computers more useful

Today, companies like IBM make real quantum hardware—a tool that scientists only began to imagine three decades ago—available to hundreds of thousands of developers. Engineers are delivering ever-more-powerful superconducting quantum processors at regular intervals, alongside crucial advances in software and quantum-classical orchestration. This work drives toward the quantum computing speed and capacity necessary to change the world.

Now that the field has achieved quantum utility, researchers are hard at work to make quantum computers even more useful. Researchers at IBM Quantum and elsewhere have identified some key challenges to improve upon quantum utility and potentially achieve quantum advantage:

1. **Scaling quantum processors:** While qubit processors used in quantum computing have the potential to massively outperform bit-based processors, current quantum processors can only support a small number of potential qubits. As research progresses, IBM plans to introduce a quantum system with 200 logical qubits capable of running 100 million quantum gates by 2029, with a goal of two thousand logical qubits capable of running 1 billion gates by 2033.
2. **Scaling quantum hardware:** Although powerful, qubits are also quite error-prone, requiring large cooling systems capable of creating temperatures lower than outer space. Researchers are currently

developing ways to scale qubits, electronics, infrastructure and software to reduce footprint, cost and energy usage.

3. **Quantum error correction:** Decoherence, the process in which qubits fail to function properly and produce inaccurate results, is a major hurdle for any quantum system. Quantum error correction requires that we encode quantum information into more qubits than we would otherwise need. In 2024, IBM announced a landmark new error-correcting code about 10 times more efficient than prior methods. While error correction is not a solved problem, this new code marks a clear path toward running quantum circuits with a billion logic gates or more.
4. **Quantum algorithm discovery:** Quantum advantage requires two components. The first is viable quantum circuits, and the second is a means to demonstrate that those quantum circuits are actually the best way to solve a quantum problem over any other state-of-the-art method. Quantum algorithm discovery is what will take current quantum technologies from quantum utility to quantum advantage.
5. **Quantum software and middleware:** The crux of quantum algorithm discovery relies on a highly performant and stable software stack to write, optimize and execute quantum programs. Open-source and Python-based, IBM's Qiskit is by far the most widely-used quantum SDK in the world—useful for executions both on IBM's fleet of superconducting quantum computers and on systems that use alternative technologies such as ions trapped in magnetic fields or quantum annealing.
6. **Quantum-centric supercomputing:** For the foreseeable future, quantum computing will work in tandem with modern and future classical supercomputing to be useful. In response, quantum researchers are preparing for a world where classical supercomputers can use quantum circuits to help solve problems.

Quantum computing components

An IBM quantum processor is a wafer not much bigger than the silicon chips found in a laptop. However, modern quantum hardware systems, used to keep the instruments at an ultracold temperature, and the extra room-temperature electronic components to control the system and process quantum data, are about the size of an average car.

While the large footprint of a complete quantum hardware system makes most quantum computers anything but portable, researchers and computer scientists are still able to access off-site quantum computing capabilities through cloud computing. The main hardware components of a quantum computer are as follows:

Quantum processors

Composed of qubits laid out in various configurations to allow for communication, quantum chips—also known as the quantum data plane—act as the brain of the quantum computer.

As the core component in a quantum computer, a quantum processor contains the system's physical qubits and the structures required to hold them in place. Quantum processing units (QPUs) include the quantum chip, control electronics and classical compute hardware required for input and output.

Superconductors

Your desktop computer likely uses a fan to get cold enough to work. Quantum processors need to be very cold—about a hundredth of a degree above absolute zero—to minimize noise and avoid decoherence to retain their quantum states. This ultra-low temperature is achieved with supercooled superfluids. At these temperatures, certain materials exhibit an important quantum mechanical effect: electrons move through them without resistance. This effect makes them superconductors.

When materials become superconductors, their electrons match up, forming Cooper pairs. These pairs can carry a charge across barriers, or insulators, through a process known as quantum tunneling. Two superconductors placed on either side of an insulator form a Josephson junction, a crucial piece of quantum computing hardware.

Control

Quantum computers use circuits with capacitors and Josephson junctions as superconducting qubits. By firing microwave photons at these qubits, we can control their behavior and get them to hold, change and read out individual units of quantum information.

Quantum software

Research continues improving quantum hardware components, but that's only one half of the equation. The crux of users' discovery of quantum advantage will be a highly performant and stable quantum software stack to enable the next generation of quantum algorithms.

In 2024, IBM introduced the first stable version of the Qiskit open source software development kit (SDK), Qiskit SDK 1.x. With over 600,000 registered users and 700 global universities that use it to develop quantum computing classes, Qiskit has become the preferred software stack for quantum computing.

But Qiskit is more than just the world's most popular quantum development software to build and construct quantum circuits. We are redefining Qiskit to represent the full-stack software for quantum at IBM, extending the Qiskit

SDK with middleware software and services to write, optimize and run programs on IBM Quantum systems—including new generative AI code-assistance tools.

Footnotes

[1] "Quantum technology sees record investments, progress on talent gap", McKinsey Digital, 24 April 2023.

Solution

IBM Quantum Safe

Quantum computers will break security protocols, but IBM Quantum Safe technology can help secure your enterprise for the quantum future.

Explore IBM Quantum Safe